Optimal Cloning of Pure States, Judging Single Clones

M. Keyl
Institut für Mathematische Physik, TU Braunschweig, Mendelssohnstr.3, 38106 Braunschweig, Germany.
Electronic Mail: m.keyl@tu-bs.de

R. F. Werner
Institut für Mathematische Physik, TU Braunschweig, Mendelssohnstr.3, 38106 Braunschweig, Germany.
Electronic Mail: R.Werner@tu-bs.de

(February 1, 2008)

We consider quantum devices for turning a finite number N of d-level quantum systems in the same unknown pure state σ into $M > N$ systems of the same kind, in an approximation of the M-fold tensor product of the state σ. In a previous paper it was shown that this problem has a unique optimal solution, when the quality of the output is judged by arbitrary measurements, involving also the correlations between the clones. We show in this paper, that if the quality judgement is based solely on measurements of single output clones, there is again a unique optimal cloning device, which coincides with the one found previously.

I. INTRODUCTION

According to the well known "no-cloning theorem" [1] perfect copying of quantum information is impossible, i.e. there is no machine which takes a quantum system as input and produces two systems of the same kind, both of them indistinguishable from the input. However, from the point of view of practical applications in Quantum Information Theory this Theorem by itself is not very useful, because it only asserts that the cloning task cannot be performed *exactly* — but then no task can be performed exactly by real devices. The fundamental importance of the No-Cloning Theorem is expressed much better in stronger versions of the Theorem, which also give explicit lower bounds on the error made in any attempt to build a cloning device. Some such bounds have been established, as well [2,3]. Even more insight into the cloning problem is given by results showing how to minimize the error, i.e., how to construct *optimal* cloning devices [4–8]. Other recent related work can be found in [9–15].

In this paper we consider cloning devices, which take as input a certain number N of identically prepared systems, and produce a larger number M of systems as output. Again, the cloning task is to make the output state resemble as much as possible a state of M systems all prepared in the same state as the inputs. This variant of the problem is of interest as a "quantum amplifier". It also has a better chance of reasonable success than a cloning device operating on single input systems: in the limit of many input systems the device can make a good statistical estimate of the input density matrix and hence produce arbitrarily good clones.

Different variants of this problem arise by different choices of the type of systems and the set of states which should be copied, e.g. pure vs. mixed states, or a finite number of states arising in a cryptographic protocol. In the present paper we are exclusively concerned with the cloning of arbitrary unknown pure states.

A second choice to be made is the precise notion of approximation between the output states of the cloning device and the (inattainable) target state. Apart from technicalities the basic issue here is whether the full states are compared, or only the one-clone marginals. Approximation in the first sense means that the expectations of all observables, including those testing correlations and entanglement between different clones, are close in the two states being compared. On the other hand, approximation in the second sense means closeness of expectations of single clone observables only. Perhaps this second condition has more of the flavour of the No-Cloning Theorem, since in that theorem, too, the requirement is that each single (!) clone be indistinguishable from the input.

In [16] we showed that the pure state cloning problem with all-particle test criterion has a unique optimal solution. In this paper we show the same for the single-particle test criterion, and that the two optimal cloning devices are actually the same. The difference between the two results may not seem great. However, the result in the present paper required much heavier mathematical machinery, and we believe it to be considerably deeper. The reason is that one-particle tests by far do not exhaust the linear space of M-particle observables. In particular, all correlations of the cloner's output are ignored by the test, which would make a *unique* optimal solution appear rather unlikely. Nevertheless, this is what we prove.

II. STATEMENT OF THE PROBLEM AND MAIN RESULT

Let us start with a precise formulation of the question we are going to consider. First of all, we will study throughout this paper only d-level systems with arbitrary but finite d. Hence the one particle Hilbert space $\mathcal{H}$ we are using is $\mathcal{H} = \mathbb{C}^d$. The Hilbert space for the input to the cloning device is therefore the N-fold tensor product $\mathcal{H}^{\otimes N}$ of $\mathcal{H}$ with itself. In fact, because we only consider tensor powers of pure states as inputs, it suffices to take the subspace of $\mathcal{H}^{\otimes N}$ spanned by vectors of the form $\varphi^{\otimes N}$ with $\varphi \in \mathcal{H}$. This is precisely the "Bose" subspace $\mathcal{H}_+^{\otimes N} \subset \mathcal{H}^{\otimes N}$, i.e., the space of vectors invariant under all permutations. The output Hilbert space will be $\mathcal{H}^{\otimes M}$ with $M > N$. On this space we cannot impose an a priori symmetry restriction, although such a restriction will come out a posteriori, as a special property of optimal cloning devices.

A *cloning map* is a completely positive, unital map $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$. This describes the action of the device on observables. Its (pre-)dual, describing the same operation in terms of states, will be denoted[1] by $T_* : \mathcal{B}_*(\mathcal{H}_+^{\otimes N}) \to \mathcal{B}_*(\mathcal{H}^{\otimes M})$. If we identify states with density operators, this means that $\mathrm{tr}\big(\rho T(A)\big) = \mathrm{tr}\big(T_*(\rho)A\big)$ for arbitrary density operators ρ and observables A. The input of the cloning device are N systems, prepared independently according to the same state σ. Thus the overall input state is $\sigma^{\otimes N}$. We will assume σ to be pure, i.e., the density matrix of σ is a one-dimensional projection onto a wave vector $\psi \in \mathcal{H}$, say. Then $\sigma^{\otimes N}$ is the projection onto the vector $\psi^{\otimes N}$. The output of the cloning device is the state $T_*(\sigma^{\otimes N})$, which is a (generally entangled) state of $M > N$ systems. Our aim is to design T so that the output states $T_*(\sigma^{\otimes N})$ approximate the product states $\sigma^{\otimes M}$.

The one particle observables, on which the comparison will be based, will be written as $a_{(k)} = \mathbb{1}^{\otimes(k-1)} \otimes a \otimes \mathbb{1}^{\otimes(M-k)} \in \mathcal{B}(\mathcal{H}^{\otimes M})$, for all $a \in \mathcal{B}(\mathcal{H})$. Thus the optimal cloning problem for arbitrary pure input states T is to make the expectations

$$\begin{aligned} &\mathrm{tr}(a_{(k)}T_*(\sigma^{\otimes N})) = \mathrm{tr}(T(a_{(k)})\sigma^{\otimes N}) = \langle \psi^{\otimes N}, T(a_{(k)})\psi^{\otimes N}\rangle \\ \text{and} \qquad &\mathrm{tr}(a_{(k)}\sigma^{\otimes M}) = \mathrm{tr}(a\sigma) = \langle \psi, a\psi\rangle \end{aligned}$$

as similar as possible for arbitrary one-particle observables a and one-particle vectors ψ. Of course, when taking a supremum over such differences, the size of a has to be constrained somehow. We will choose the constraint $0 \le a \le \mathbb{1}$, which is to say that the above two expressions have an immediate interpretation as probabilities. The largest difference of such probabilities is now the error functional for cloning maps, which we will seek to minimize:

$$\Delta_{\mathrm{one}}(T) = \sup_{a,\psi,k} \big|\langle \psi^{\otimes N}, T(a_{(k)})\psi^{\otimes N}\rangle - \langle \psi, a\psi\rangle\big| \tag{1}$$

where the supremum is taken over all $\psi \in \mathcal{H}$ with $\|\psi\| = 1$, all operators $a \in \mathcal{B}(\mathcal{H})$ with $0 \le a \le \mathbb{1}$, and all integers $1 \le k \le M$.

The corresponding quantity based on tests of the full output state (including correlations) is

$$\Delta_{\mathrm{all}}(T) = \sup_{A} \sup_{\sigma,\mathrm{pure}} \left|\mathrm{tr}\left(T(A)\sigma^{\otimes N}\right) - \mathrm{tr}(A\sigma^{\otimes M})\right|,$$

where the supremum is taken over all $A \in \mathcal{B}(\mathcal{H}^{\otimes M})$ with $0 \le A \le \mathbb{1}$ and over all pure states $\sigma \in \mathcal{B}_*(\mathcal{H})$. Due to the properties of the trace norm $\|\cdot\|_1$ this functional can be expressed by

$$\Delta_{\mathrm{all}}(T) = \sup_{\sigma,\mathrm{pure}} \|T_*(\sigma^{\otimes N}) - \sigma^{\otimes M}\|_1. \tag{2}$$

It turns out that there is exactly one cloning map $\widehat{T}$ which minimizes this error functional. This can be proven with a minor adaptation of the arguments in [16], which start from a slightly different criterion, namely the maximization of the "fidelity" $\mathcal{F}(T_*) = \sup_{\sigma,\mathrm{pure}}(\sigma^{\otimes M}T_*(\sigma^{\otimes N}))$. The unique solution $T = \widehat{T}$ minimizing (2), or maximizing $\mathcal{F}(T_*)$, is best expressed in terms of its action on states, i.e.,

$$\widehat{T}_*(\rho) = \frac{d[N]}{d[M]} S_M(\rho \otimes \mathbb{1}^{M-N})S_M. \tag{3}$$

[1] In [16] the symbol T was used for T_*. In contrast to [16] the key arguments in the present paper are phrased more readily in terms of the map on observables than in terms of the map on states. Therefore, we decided to change this notation, which then also agrees better with the usage for completely positive maps on operator algebras.

Here $d[N] = \binom{d+N-1}{N}$ denotes the dimension of the symmetric subspace $\mathcal{H}_+^{\otimes N}$, S_M is the projection from $\mathcal{H}^{\otimes M}$ to $\mathcal{H}_+^{\otimes M}$, and ρ is an arbitrary density operator on $\mathcal{H}_+^{\otimes N}$. In [16] we also computed the one-site restriction of the output states of this cloner:

$$\operatorname{tr}\left(\widehat{T}(a_k)\sigma^{\otimes N}\right) = \gamma(\widehat{T})\sigma(a) + (1-\gamma(\widehat{T}))\operatorname{tr}(a)/d \quad ,$$

where

$$\gamma(\widehat{T}) = \frac{N}{N+d}\,\frac{M+d}{M}$$

is the so-called Black Cow factor of $\widehat{T}$, interpreted as a "shrinking factor of the Poincaré sphere" in the discussions of the qubit ($d=2$) case. This makes it easy to verify the case of equality in the following Theorem, which is our main result.

1 Theorem. *For any cloning map $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ we have*

$$\Delta_{\text{one}}(T) \geq \frac{d-1}{d}\left|1 - \frac{N}{N+d}\,\frac{M+d}{M}\right|$$

with equality iff $T = \widehat{T}$ with $\widehat{T}$ from equation (3).

III. FINDING THE OPTIMAL CLONING MAP

A. Reduction to the covariant case

In this section we will give the proof of our main theorem, apart from some group theoretical Lemmas, which will be proved in Appendix A. Throughout, the symmetry of sitewise unitary rotation of clones and input states will play a crucial role. The necessary background information on unitary representations of SU(d) will also be supplied in Appendix A.

We establish some notation first. By U(d) we will denote the group of unitary $d \times d$-matrices, i.e., the unitary group on our underlying one-particle space $\mathcal{H} \equiv \mathbb{C}^d$. Unitary representations of this group will be denoted by the letter π with suitable indices. $\pi_\square$ is the defining representation on $\mathbb{C}^d$, and its n^{th} tensor power, acting on $\mathcal{H}^{\otimes N}$ by the operators $\pi_\square^{\otimes N}(u) = u^{\otimes N}$ is $\pi_\square^{\otimes N}$. The restriction of this representation to the symmetric subspace $\mathcal{H}_+^{\otimes N}$ will be denoted by π_N^+. Thus a cloning map $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ is called U(d)-*covariant*, if

$$T\left(\pi_\square^{\otimes M}(u) A \pi_\square^{\otimes M}(u)^*\right) = \pi_N^+(u) T(A) \pi_N^+(u)^* \tag{4}$$

This equation merely expresses that T does not prefer any direction in $\mathcal{H}$. It would be a natural initial assumption for good cloning devices but, of course, in our case it will come out as a result of the minimization: $\widehat{T}$ from equation (3) is obviously covariant, because S_M commutes with all $\pi_\square^{\otimes M}(u)$. It is convenient to state the covariance condition as a fixed point property: we define the action τ of unitary rotations on cloning maps by

$$(\tau_u T)(A) = \pi_N^+(u)^* T\left(\pi_\square^{\otimes M}(u) A \pi_\square^{\otimes M}(u)^*\right)\pi_N^+(u), \tag{5}$$

so that T is covariant iff $\tau_u(T) = T$ for all $u \in \mathrm{U}(d)$. We denote by $\overline{T}$ the average of $\tau_u T$ with respect to u, i.e.,

$$\overline{T} = \int du\ \tau_u(T), \tag{6}$$

where "du" denotes the normalized Haar measure on U(d).

The fact that the cloning error Δ_{one} does not single out a direction on $\mathcal{H}$ either is expressed by the — easily verified — equation

$$\Delta_{\text{one}}(\tau_u T) = \Delta_{\text{one}}(T). \tag{7}$$

Similarly, we can get an estimate of $\Delta_{\rm one}(\overline{T})$: The functional $\Delta_{\rm one}$ is defined as the supremum of a set of convex expressions in T. Therefore, it is convex, and $\Delta_{\rm one}(\overline{T}) \leq \Delta_{\rm one}(T)$. So as long as we are only interested in finding *some* cloning map with minimal $\Delta_{\rm one}$, we may restrict attention to covariant ones.

There is a similar simplification, which we can make "without loss of cloning quality": $\Delta_{\rm one}$ is invariant under a change of the ordering of the clones. That is to say, if $V : \mathcal{H}^{\otimes M} \to \mathcal{H}^{\otimes M}$ is a permutation operator, and if we define $\tau_V T$ by $(\tau_V T)(A) = T(VAV^*)$, we may replace T by its average over permutations without loss of cloning quality. That is, we may assume that $\tau_V T = T$ for all permutations V. We will refer to this property as *permutation invariance*.

Our strategy is now to assume $\mathrm{U}(d)$-covariance and permutation invariance of T, and to show that there is a unique solution to the variational problem with these additional properties. The above convexity argument then implies that no other cloning map can do better. But since the functional $\Delta_{\rm one}$ is not strictly convex, we will need an extra step to establish uniqueness. This we will do in subsection III F by showing that any cloning map whose mean is the optimal covariant cloner has to be covariant itself.

B. Reduction to the extremal covariant case

The functional $\Delta_{\rm one}$ involves only operators $T(A)$ with A of the special form $A = a_{(k)} = \mathbb{1}^{\otimes(k-1)} \otimes a \otimes \mathbb{1}^{\otimes(M-k)} \in \mathcal{B}(\mathcal{H}^{\otimes M})$. Now due to permutation invariance $T(a_{(k)})$ does not depend on k, and we have

$$T(a_{(k)}) = \frac{1}{M} T\Big(\sum_k a_{(k)}\Big). \tag{8}$$

What makes this equation useful is that on the right hand side T is now applied to one of the generators of the representation $\pi_\square^{\otimes N}$: we have $\exp\big(i \sum_{k=1}^M a_{(k)}\big) = \big(\exp(ia)\big)^{\otimes M}$. Because T is covariant, we can determine how the operators in equation (8) transform under $\mathrm{U}(d)$-rotations:

$$\pi_N^+(u) T(a_{(k)}) \pi_N^+(u)^* = T\big((uau^*)_{(k)}\big), \tag{9}$$

where the multiplication of a and u on the right hand side is in the $d \times d$-matrices. This property fixes the "transformation behaviour" of the operators $T(a_{(k)})$, and as we will see, this essentially fixes the tuple of operators $T(a_{(k)})$. Of course, $a = \mathbb{1}$ in (9) simply leads to $T(\mathbb{1}_{(k)}) = T(\mathbb{1}) = \mathbb{1}$. The operator $i\mathbb{1}$ is the (anti-hermitian) generator of the subgroup of unitaries multiplying each vector with the same phase. More interesting are the generators of $\mathrm{SU}(d)$, in which such trivial phases have been eliminated. These generators, in other words the Lie algebra $\mathfrak{su}(d)$, are exactly the traceless anti-hermitian $d \times d$-matrices. In the qubit case ($d = 2$) $\mathfrak{su}(2)$ is spanned by the Pauli matrices (multiplied by i), and 3-tuples of operators transforming like the generators are known in physics literature as "vector operators". It is well-known that, due to the simple reducibility of $\mathrm{SU}(2)$, each irreducible representation of $\mathrm{SU}(2)$ contains exactly one vector operator (up to a factor), namely the generators (angular momentum operators) of the representation themselves. So all operators $T(a_{(k)})$ are determined by the single numerical factor relating the operators $T(a_{(k)})$ to the generators of the irreducible representation π_N^+.

It turns out that the same idea works in the $\mathrm{SU}(d)$-case for arbitrary d. In order to state it precisely, we need a notation for the Lie algebra representation associated with a unitary representation of a Lie group. We define $\partial\pi(X)$ to be the anti-hermitian generator of the one-parameter subgroup generated by X, i.e.,

$$\partial\pi(X) = \frac{d}{dt} \pi\big(e^{tX}\big)\Big|_{t=0}. \tag{10}$$

Then the desired property of a representation is stated in the following definition:

2 Definition. *Let $\pi : G \to \mathcal{B}(\mathcal{H}_\pi)$ be a finite dimensional unitary representation of a Lie group G with Lie algebra $\mathfrak{g}$. Then $\mathfrak{g}$ is said to be* **non-degenerate** *in $\mathcal{B}(\mathcal{H}_\pi)$ with respect to π, if any linear operator $L : \mathfrak{g} \to \mathcal{B}(\mathcal{H}_\pi)$ with the covariance property $\pi(g)L(X)\pi(g)^* = L(gXg^{-1})$ is of the form $L(X) = \lambda\partial\pi(X)$, for some factor $\lambda \in \mathbb{C}$.*

As we argued above, $\mathfrak{su}(2)$ is non-degenerate in *every* irreducible representation of $\mathrm{SU}(2)$. However, for $d \geq 3$ we can find representations containing degenerate copies of the generators, and we have to make sure that the special representations occurring in the present problem are of the "good" kind. This is the content of the following Lemma, proved in Appendix A.

3 Lemma. *$\mathfrak{su}(d)$ is non-degenerate in $\mathcal{B}(\mathcal{H}_+^{\otimes N})$ with respect to π_N^+.*

4 Corollary. *Let $\pi : \mathrm{U}(d) \to \mathcal{B}(\mathcal{H}_\pi)$ be a unitary representation, and let $T : \mathcal{B}(\mathcal{H}_\pi) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ be a completely positive normalized and $\mathrm{U}(d)$-covariant map, i.e. $T(\pi(u)A\pi(u)^*) = \pi_N^+(u)T(A)\pi_N^+(u)^*$. Then there is a number $\omega(T)$ such that*

$$T(\partial\pi(a)) = \omega(T)\sum_{k=1}^{N} a_{(k)},$$

for every $a \in \mathcal{B}(\mathcal{H})$ with $\mathrm{tr}(a) = 0$.

Given $\omega(T)$ for $\pi = \pi_\square^{\otimes M}$, we can compute the cloning error $\Delta_{\mathrm{one}}(T)$ as follows: given $a \in \mathcal{B}(\mathcal{H})$ with $0 \leq a \leq \mathbb{1}$, we can write $a = \alpha\mathbb{1} + a'$ with $\mathrm{tr} a' = 0$. Then

$$\begin{aligned} T(a_{(k)}) &= \alpha\mathbb{1} + \frac{1}{M}T\Big(\sum_{l=1}^{M} a'_{(l)}\Big) \\ &= \alpha\mathbb{1} + \frac{\omega(T)}{M}\Big(\sum_{l=1}^{N} a'_{(l)}\Big) \end{aligned}$$

and with $a' = a - \alpha\mathbb{1}$ and $\alpha = \frac{\mathrm{tr}\, a}{d}$

$$T(a_{(k)}) = \frac{\mathrm{tr}\, a}{d}\left(1 - \frac{N\omega(T)}{M}\right)\mathbb{1} + \frac{\omega(T)}{M}\left(\sum_{l=1}^{N} a_{(l)}\right).$$

In any state $\psi \in \mathcal{H}$ we get

$$\langle\psi, a\psi\rangle - \langle\psi^{\otimes N}, T(a_{(k)})\psi^{\otimes N}\rangle = (1 - \gamma(T))\left(\langle\psi, a\psi\rangle - \frac{\mathrm{tr}\, a}{d}\right)$$

where $\gamma(T) = \frac{N}{M}\omega(T)$ is the Black-Cow factor already mentioned in Section II. With

$$\sup_{\psi, a}\left(\langle\psi, a\psi\rangle - \frac{\mathrm{tr}\, a}{d}\right) = \frac{d-1}{d}$$

we get

$$\Delta_{\mathrm{one}}(T) = \frac{d-1}{d}\left|1 - \frac{N}{M}\omega(T)\right| = \frac{d-1}{d}\left|1 - \gamma(T)\right|. \tag{11}$$

We remark that the largest possible $\omega(T)$, to be determined below, still makes the second term in the absolute value less than 1, so we could omit the absolute value signs. In any case, we will only seek to maximize $\omega(T)$ from now on, ignoring the possibility of $\omega(T) > M/N$, anticipating that it will be ruled out by the result of the maximization anyway.

An important observation about the Corollary and formula (11) is that ω is clearly an *affine* functional on the convex set of covariant cloning maps (i.e., ω respects convex combinations). Whereas we previously used the convexity of Δ_{one} to conclude that averaging over rotations and permutations (and hence a move towards the interior of the convex set of cloning maps) generally improves the cloning quality, we now see that the optimum can be sought, as for any affine functional, on the extreme boundary of the subset of covariant cloning maps. Therefore our next steps will be aimed at the determination of the extremal $\mathrm{U}(d)$-covariant and permutation invariant cloning maps, and, subsequently the solution of the variational problem for these extremal cases.

C. Convex decomposition of covariant cloning maps

For the first reduction step we use the close connection between the permutation operators on $\mathcal{H}^{\otimes M}$ and the representation $\pi_\square^{\otimes M}$. Let $\left(\pi_\square^{\otimes M}\right)'$ denote the algebra of all operators on $\mathcal{H}^{\otimes M}$ commuting with all $\pi_\square^{\otimes M}(u) \equiv u^{\otimes M}$. This algebra consists precisely of the linear combinations of permutation unitaries [17, Theorem IX.11.5]. So consider a reduction of $\pi_\square^{\otimes M}$ into irreducibles, i.e., an orthogonal decomposition of the identity into minimal projections $E_\alpha \in$

$(\pi_{\square}^{\otimes M})'$. Then due to covariance the operators $T(E_\alpha)$ commute with all $\pi_N^+(u)$, and because the latter representation is irreducible, they must be multiples of the identity, $T(E_\alpha) = r_\alpha \mathbb{1}$, say. Because $T(VA) = T(AV)$ for permutation operators V, we also have $T(AE_\alpha) = T(E_\alpha A E_\alpha)$. Hence

$$T_\alpha(A) = r_\alpha^{-1} T(E_\alpha A E_\alpha) \tag{12}$$

is a legitimate cloning map in its own right (provided $r_\alpha \neq 0$). Moreover,

$$T(A) = \sum_\alpha T(AE_\alpha) = \sum_\alpha T(E_\alpha A E_\alpha) = \sum_\alpha r_\alpha T_\alpha(A) \tag{13}$$

is a convex decomposition of the given T into such summands. Maximizing $\omega(T) = \sum_\alpha r_\alpha \omega(T_\alpha)$ thus means concentrating the coefficients r_α on those α, for which $\omega(T_\alpha)$ is maximal. At this stage it is perhaps already plausible that only the summand T_α, for which $E_\alpha = S_M$ is the projection onto the symmetric subspace will give the best $\omega(T_\alpha)$, because this is the space supporting the pure states $\sigma^{\otimes M}$ the cloner is supposed to approximate. In fact, for the optimization of Δ_{all} in [16] this idea leads directly to a simple solution. In the present case we found no direct proof of this plausible statement.

We therefore have to enter into the further convex decomposition of each T_α. The output states of this cloning map are supported by $\mathcal{H}_\alpha \equiv E_\alpha \mathcal{H}^{\otimes M}$, and we will restrict T_α accordingly, i.e., we consider it as a covariant map $T_\alpha : \mathcal{B}(\mathcal{H}_\alpha) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$, which is covariant with respect to the restricted representation $\pi_\alpha = \pi^{\otimes M} \restriction \mathcal{H}_\alpha$ and π_N^+.

As for any completely positive map, the convex decompositions of T_α are governed by the Stinespring dilation [18]. Since we are looking, more specifically, for decompositions into covariant completely positive maps, we have to invoke a "covariant" version of the Stinespring dilation Theorem [19], which is stated in Appendix B for the convenience of the reader. According to this Theorem we can write a covariant completely positive $T_\alpha : \mathcal{B}(\mathcal{H}_\alpha) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ as $T_\alpha(A) = V^*(A \otimes \mathbb{1}_\mathcal{K})V$, where $\mathcal{K}$ is some auxiliary Hilbert space carrying a unitary representation $\widetilde{\pi} : \mathrm{U}(d) \to \mathcal{B}(\mathcal{K})$, and $V : \mathcal{H}_+^{\otimes N} \to \mathcal{H}_\alpha \otimes \mathcal{K}$ is an isometry intertwining the respective representations, i.e.,

$$V\pi_N^+(u) = \big(\pi_\alpha(u) \otimes \widetilde{\pi}(u)\big)V. \tag{14}$$

The convex reduction theory of T_α is now the same as the reduction theory of $\widetilde{\pi}$ into irreducibles: if F_β is a minimal projection in the algebra $\widetilde{\pi}'$, and hence $\widetilde{\pi} \restriction F_\beta \mathcal{K}$ is irreducible, then $A \mapsto V^*(A \otimes F_\beta)V$ is a covariant map, which cannot be further decomposed into a sum of covariant completely positive maps (see Appendix B). Note that $V^*(\mathbb{1} \otimes F_\beta)V$ commutes with the irreducible representation π_N^+, so that once again this summand is normalized up to a factor: $V^*(\mathbb{1} \otimes F_\beta)V = r_\beta \mathbb{1}$. Therefore $T_\alpha = \sum_\beta r_\beta T_{\alpha\beta}$, where each $T_{\alpha\beta}(A) = r_\beta^{-1} V^*(A \otimes F_\beta)V$ is again an admissible cloning map. The following statement summarizes the result of the decomposition theory of T.

5 Proposition. *Let $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ be a $\mathrm{U}(d)$-covariant and permutation invariant cloning map. Then T is a convex combination $T = \sum_{\alpha\beta} r_{\alpha\beta} T_{\alpha\beta}$ such that each $T_{\alpha\beta}$ is of the following special form: $T_{\alpha\beta}(A) = V^*(A \otimes \mathbb{1}_\beta)V$, where V is an intertwining isometry between π_N^+ and $\pi_\alpha \otimes \pi_\beta$, such that $\pi_\alpha : \mathrm{U}(d) \to \mathcal{B}(\mathcal{H}_\alpha)$ is an irreducible subrepresentation of $\pi_{\square}^{\otimes M}$, and $\pi_\beta : \mathrm{U}(d) \to \mathcal{B}(\mathcal{H}_\beta)$ is also an irreducible unitary representation.*

This Proposition summarizes all that is needed for the further treatment of the variational problem. However, we could have made a slightly stronger statement by eliminating the non-uniqueness introduced by the choice of the minimal projections E_α. If the subrepresentations π_α and $\pi_{\alpha'}$ are unitarily equivalent, then they can be connected by a unitary, which is again a linear combination of permutations. Hence the contribution of the term $r_\alpha T_\alpha = \sum_\beta r_{\alpha\beta} T_{\alpha\beta}$ to $\omega(T)$ depends only on the isomorphism type of π_α.

What we cannot assert in general, however, is that V is determined by the isomorphism types of π_α and π_β: among the groups $\mathrm{SU}(d)$ only $d = 2$ is "simply reducible", which means that the space of intertwiners between π_γ and $\pi_\alpha \otimes \pi_\beta$ is at most one-dimensional for arbitrary irreducible representations $\pi_\alpha, \pi_\beta, \pi_\gamma$. In the following subsection we will therefore focus on the qubit case, and show how to determine $\omega(T_{\alpha\beta})$ from the representations involved. This procedure will then be generalized to arbitrary d, and it will turn out that, perhaps surprisingly, in the general case $\omega(T_{\alpha\beta})$ also depends on π_α, π_β only up to unitary equivalence.

D. Maximizing ω in the case $d = 2$

For $d = 2$ the representations of $\mathrm{SU}(2)$ are conventionally labelled by their "total angular momentum" $j = 0, 1/2, 1, \ldots$. The irreducible representation π_j has dimension $2j + 1$, and is isomorphic to π_N^+ with $N = 2j$ in the notation used above. For $j = 1$ we get the 3-dimensional representation isomorphic to the rotation group, which is

responsible for the importance of this group in physics. In a suitable basis X_1, X_2, X_3 of the Lie algebra $\mathfrak{su}(2)$ we get the commutation relations $[X_1, X_2] = X_3$, and cyclic permutations of the indices thereof. In the $j = 1$ representation $\partial\pi_1(X_k)$ generates the rotations around the k-axis in 3-space. The Casimir operator of SU(2) is the square of this vector operator, i.e., $\widetilde{\mathbf{C}}_2 = \sum_{k=1}^3 X_k^2$. In the representation π_j it is the scalar $j(j+1)$, i.e., if we extend the representation $\partial\pi$ of the Lie algebra to the universal enveloping algebra (which also contains polynomials in the generators), we get $\partial\pi_j(\widetilde{\mathbf{C}}_2) = j(j+1)\mathbb{1}$. We can use this to determine $\omega(T_{\alpha\beta})$ for arbitrary irreducible representations. This computation can be seen as an elementary computation of a so-called $6j$-symbol (see also [20] for a context in which the same computation arises), but we will not need to invoke any of the $6j$-machinery.

So let V be an intertwining isometry between π_γ and $\pi_\alpha \otimes \pi_\beta$, where $\alpha, \beta, \gamma \in \{0, 1/2, \ldots\}$ label irreducible representations. Then ω is defined by

$$\omega \cdot \partial\pi_\gamma(X_k) = V^*(\partial\pi_\alpha(X_k) \otimes \mathbb{1}_\beta)V. \tag{15}$$

We multiply this equation by $\partial\pi_\gamma(X_k)$, use the intertwining property of V in the form $V\partial\pi_\gamma(X) = \big(\partial\pi_\alpha(X) \otimes \mathbb{1}_\beta + \mathbb{1}_\alpha \otimes \partial\pi_\beta(X)\big)V$, and sum over k to get

$$\omega \cdot \partial\pi_\gamma(\widetilde{\mathbf{C}}_2) = V^*\big(\partial\pi_\alpha(\widetilde{\mathbf{C}}_2) \otimes \mathbb{1}_\beta\big)V + \sum_k V^*\big(\partial\pi_\alpha(X_k) \otimes \partial\pi_\beta(X_k)\big)V. \tag{16}$$

The tensor product in the second summand can be re-expressed in terms of Casimir operators as

$$\sum_k \big(\partial\pi_\alpha(X_k) \otimes \partial\pi_\beta(X_k)\big) = \frac{1}{2}\sum_k \big(\partial\pi_\alpha(X_k) \otimes \mathbb{1}_\beta + \mathbb{1}_\alpha \otimes \partial\pi_\beta(X_k)\big)^2 - \frac{1}{2}\partial\pi_\alpha(\widetilde{\mathbf{C}}_2) \otimes \mathbb{1}_\beta - \frac{1}{2}\mathbb{1}_\alpha \otimes \partial\pi_\alpha(\widetilde{\mathbf{C}}_2).$$

Inserting this into the previous equation, using the intertwining property once again, and inserting the appropriate scalars for $\partial\pi(\widetilde{\mathbf{C}}_2) \equiv \widetilde{C}_2(\pi)\mathbb{1}$, we find that $\omega \cdot \widetilde{C}_2(\pi_\gamma) = \widetilde{C}_2(\pi_\alpha) + \frac{1}{2}\big(\widetilde{C}_2(\pi_\gamma) - \widetilde{C}_2(\pi_\alpha) - \widetilde{C}_2(\pi_\beta)\big)$, and hence

$$\omega = \frac{1}{2} + \frac{\widetilde{C}_2(\pi_\alpha) - \widetilde{C}_2(\pi_\beta)}{2\widetilde{C}_2(\pi_\gamma)}. \tag{17}$$

Note that we have only used the fact that the Casimir operator $\widetilde{\mathbf{C}}_\mathbf{2}$ is some fixed quadratic expression in the generators. This is also true for SU(d). Hence equation (17) also holds in the general case. In particular, we have shown that for the purpose of optimizing $\omega(T_{\alpha\beta})$ only the isomorphism types of π_α and π_β are relevant, but not the particular intertwiner V.

Specializing again to the case $d = 2$, we find

$$\omega = \frac{1}{2} + \frac{\alpha(\alpha+1) - \beta(\beta+1)}{2\gamma(\gamma+1)}. \tag{18}$$

Here $\gamma = N/2$ is fixed by the number N of input systems. α is constrained by the condition that π_α must be a subrepresentation of $\pi_{j=1/2}^{\otimes M}$, which is equivalent to $\alpha \leq M/2$. Finally, β is constrained by the condition that there must be a non-zero intertwiner between π_γ and $\pi_\alpha \otimes \pi_\beta$. It is well-known that this condition is equivalent to the inequality $|\alpha - \beta| \leq \gamma \leq \alpha + \beta$. This is the same as the "triangle inequality": the sum of any two of α, β, γ is larger than the third. The area of admissible pairs (α, β) is represented in Fig. 1.

Since $x \mapsto x(x+1)$ is increasing for $x \geq 0$, we maximize ω with respect to β in equation (18) if we choose β as small as possible, i.e., $\beta = |\alpha - \gamma|$. Then the numerator in equation (18) becomes

$$\alpha(\alpha+1) - \beta(\beta+1) = 2\alpha\gamma - \gamma^2 + \max\{\gamma, 2\alpha - \gamma\},$$

which is strictly increasing in α. Hence the maximum

$$\omega_{\max} = \frac{M+2}{N+2} \tag{19}$$

is attained for and only for $\alpha = M/2$ and $\beta = (M-N)/2$.

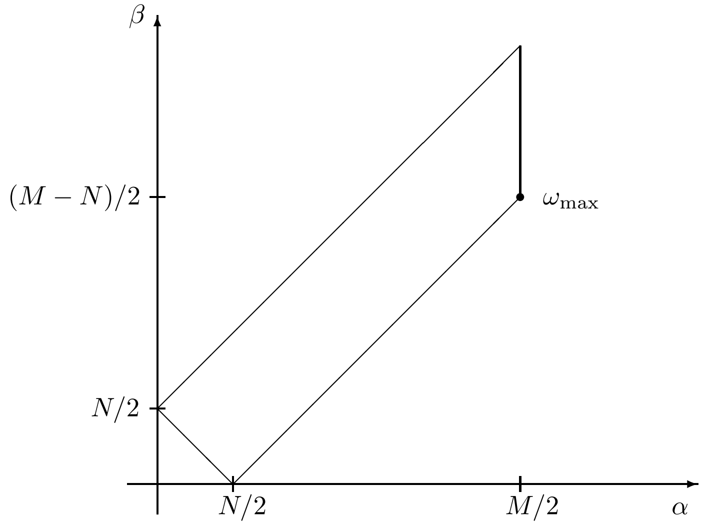

FIG. 1. Area of admissible pairs (α, β).

Note that the seemingly simpler procedure of first maximizing α and then minimizing β to the smallest value consistent with $\alpha = M/2$ leads to the same result, but is fallacious because it fails to rule out possibly larger values of ω in the lower triangle of the admissible region in Fig. 1. The same problem arises for higher d, and one has to be careful to find a maximization procedure which takes into account all constraints.

E. Maximizing ω in the general case

Let us generalize now the previous discussion to arbitrary but finite d. In this case irreducible representations of $\mathrm{U}(d)$ are labelled, according to Section A 2 by their highest weight $\mathbf{m} = (m_1, \dots, m_d)$. Hence we can decompose $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ as described in Prop. 5 into the sum $T = \sum_{(\mathbf{m},\mathbf{n}) \in W} r_{\mathbf{m},\mathbf{n}} T_{\mathbf{m},\mathbf{n}}$, taken over the set

$$W = \{(\mathbf{m}, \mathbf{n}) \in \mathbb{Z}_+^d \times \mathbb{Z}_+^d \,|\, \pi_{\mathbf{m}} \subset \pi_{\square}^{\otimes M} \text{ and } \pi_N^+ \subset \pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}}\}.$$

Here $\mathbb{Z}_+^d$ is an abbreviation for the set of all possible weights of irreducible $\mathrm{U}(d)$ representations, i.e. $\mathbb{Z}_+^d = \{(m_1, \dots, m_d) \,|\, m_1 \geq m_2 \geq \dots \geq m_d\}$.

Our task is now to determine $(\mathbf{m}, \mathbf{n}) \in W$ such that $\omega = \omega(T_{\mathbf{m},\mathbf{n}})$ becomes maximal. To this end we consider in analogy to (15) the equation

$$\omega \cdot \partial\pi_N^+(X) = V^*(\partial\pi_{\mathbf{m}}(X) \otimes \mathbb{1}_{\mathbf{n}})V, \quad \forall X \in \mathfrak{su}(d) \tag{20}$$

where V is an intertwining isometry between π_N^+ and $\pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}}$. Note that equation (20) is valid only for $X \in \mathfrak{su}(d)$ (and not for $X \in \mathfrak{u}(d)$ in general). Hence we have to consider the second order Casimir operator $\widetilde{\mathbf{C}}_2$ of $\mathrm{SU}(d)$ which is given, according to Appendix A 5, by an expression of the form $\widetilde{\mathbf{C}}_2 = \sum_{jk} g^{jk} X_j X_k$. This is all we needed in the derivation of equation (17) in the SU(2)-case. The generalization to arbitrary d hence reads

$$\omega = \frac{1}{2} + \frac{\widetilde{C}_2(\pi_{\mathbf{m}}) - \widetilde{C}_2(\pi_{\mathbf{n}})}{2\widetilde{C}_2(\pi_N^+)} \quad . \tag{21}$$

The concrete form of $\widetilde{C}_2(\pi_{\mathbf{m}})$ as a function of the weights $\mathbf{m}$ is given in equation (A8), and will be needed only later. Since $\widetilde{C}_2(\pi_N^+)$ is a positive constant we have to maximize the function

$$W \ni (\mathbf{m}, \mathbf{n}) \mapsto F(\mathbf{m}, \mathbf{n}) = \widetilde{C}_2(\pi_{\mathbf{m}}) - \widetilde{C}_2(\pi_{\mathbf{n}}) \in \mathbb{Z} \tag{22}$$

on its domain W.

The first step in this direction is to reexpress $F(\mathbf{m}, \mathbf{n})$ in terms of the $\mathrm{U}(d)$ Casimir operators $\mathbf{C}_2$ and $\mathbf{C}_1^2$. Note in this context that although equation (20) is, as already stated, valid only for $X \in \mathfrak{su}(d)$ the representations $\pi_{\mathbf{m}}$ and $\pi_{\mathbf{n}}$ are still $\mathrm{U}(d)$ representations Hence we can apply the equation $\widetilde{\mathbf{C}}_2 = \mathbf{C}_2 - \frac{1}{d}\mathbf{C}_1^2$ given in Section A 5:

$$F(\mathbf{m},\mathbf{n}) = C_2(\pi_{\mathbf{m}}) - C_2(\pi_{\mathbf{n}}) - \frac{1}{d}(C_1^2(\pi_{\mathbf{m}}) - C_1^2(\pi_{\mathbf{n}})). \tag{23}$$

This rewriting is helpful, because the invariants C_1 turn out to be independent of the variational parameters: Since $\pi_{\mathbf{m}} \subset \pi_{\square}^{\otimes M}$, and $\partial\pi_{\square}^{\otimes M}(\mathbb{1}_d) = M\mathbb{1}$, we also have $C_1(\pi_{\mathbf{m}}) = M$. On the other hand, the existence of an intertwining isometry V with $V\pi_N^+ = \pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}} V$ implies

$$VC_1(\pi_N^+)\mathbb{1} = V\partial\pi_N^+(\mathbf{C}_1) = (\partial\pi_{\mathbf{m}}(\mathbf{C}_1) \otimes \mathbb{1}_{\mathbf{n}} + \mathbb{1}_{\mathbf{m}} \otimes \partial\pi_{\mathbf{n}}(\mathbf{C}_1))\, V = (C_1(\pi_{\mathbf{m}})\mathbb{1} + C_1(\pi_{\mathbf{n}})\mathbb{1})\, V$$

and therefore $C_1(\pi_N^+) = C_1(\pi_{\mathbf{m}}) + C_1(\pi_{\mathbf{n}})$. Since $C_1(\pi_N^+) = N$ and $C_1(\pi_{\mathbf{m}}) = M$ we get $C_1(\pi_{\mathbf{n}}) = N - M$. Inserting this into equation (23) we find the functional

$$F(\mathbf{m},\mathbf{n}) = F_1(\mathbf{m},\mathbf{n}) - \frac{2MN - N^2}{d}, \tag{24}$$

where only F_1 depends on the variational parameters, and is expressed explicitly (see equation A7) as

$$W \ni (\mathbf{m},\mathbf{n}) \mapsto F_1(\mathbf{m},\mathbf{n}) = C_2(\pi_{\mathbf{m}}) - C_2(\pi_{\mathbf{n}}) = \sum_{j=1}^{d}(m_j^2 - n_j^2) + \sum_{k=1}^{d}(d - 2k + 1)(m_k - n_k) \in \mathbb{Z} \tag{25}$$

which remains to be maximized over W.

To do this we have to express the constraints defining the domain W more explicitly. We have already seen that $\mathbf{m} \in \mathbb{Z}_+^d$ has to satisfy the constraint $\sum_{j=1}^d m_j = M$. In addition we get, due to equation A1 $m_d > 0$. To fix the constraints for $\mathbf{n}$ note that according to equation (A4) $\pi_N^+ \subset \pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}}$ is equivalent to $\pi_{\mathbf{m}} \subset \pi_N^+ \otimes \pi_{\widetilde{\mathbf{n}}}$. Here we have introduced $\widetilde{\mathbf{n}} = (\widetilde{n}_1, \ldots, \widetilde{n}_d) = (-n_d, \ldots, -n_1)$ as a notation for the highest weight of the representation $\overline{\pi_{\mathbf{n}}}$ conjugate to $\pi_{\mathbf{n}}$ (i.e. $\overline{\pi_{\mathbf{n}}} = \pi_{\widetilde{\mathbf{n}}}$). Now we can apply equation (A3) to get

$$\pi_N^+ \subset \pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}} \iff \widetilde{n}_k = m_k - \mu_k \text{ with } 0 \leq \mu_k \leq m_k - m_{k+1}\ \forall k = 1, \ldots, d-1 \text{ and } \sum_{k=1}^{d} \mu_k = N.$$

In other words

$$W = \{(\mathbf{m},\mathbf{n}) \,|\, \widetilde{\mathbf{n}} = \mathbf{m} - \mu, \text{ and } (\mathbf{m},\mu) \in W_1\}$$

with

$$W_1 = \{(\mathbf{m},\mu) \in \mathbb{Z}_+^d \times \mathbb{Z}^d \,|\, \sum_{k=1}^{d} m_k = M,\ \sum_{k=1}^{d} \mu_k = N \text{ and } 0 \leq \mu_k \leq m_k - m_{k+1}\ \forall k = 1, \ldots, d-1\}.$$

The function F_1 can now be re-expressed in terms the new variables $(\mathbf{m},\mu)$. To this end note that $C_2(\pi_{\mathbf{n}}) = C_2(\overline{\pi_{\mathbf{n}}}) = C_2(\pi_{\widetilde{\mathbf{n}}})$. Hence we have

$$F_1(\mathbf{m},\mathbf{n}) = F_1(\mathbf{m},\widetilde{\mathbf{n}}) = F_1(\mathbf{m},\mathbf{m} - \mu)$$

and therefore with equation (25):

$$F_1(\mathbf{m},\widetilde{\mathbf{n}}) = \sum_{k=1}^{d} \mu_k(2m_k - 2k - \mu_k) + (d+1)\sum_{k=1}^{d} \mu_k = F_2(\mathbf{m},\mu) + (d+1)N \tag{26}$$

with the new function

$$W_1 \ni (\mathbf{m},\mu) \mapsto F_2(\mathbf{m},\mu) = \sum_{k=1}^{d} \mu_k(2m_k - 2k - \mu_k) \in \mathbb{Z}. \tag{27}$$

Hence we have reduced our problem to the following Lemma:

6 Lemma. *The function $F_2 : W_1 \to \mathbb{Z}$ defined in equation (27) attains its maximum for and only for*

$$\mathbf{m}_{\max} = (M, 0, \ldots, 0) \qquad \textit{and} \qquad \mu_{\max} = \begin{cases} (N, 0, \ldots, 0) & \textit{for } N \leq M \\ (M, 0, \ldots, 0, N-M) & \textit{for } N \geq M. \end{cases}$$

Proof: We consider a number of cases in each of which we apply a different strategy for increasing F_2. In these procedures we consider d to be a variable parameter, too, because if $\mu_d = m_d = 0$, the further optimization will be treated as a special case of the same problem with d reduced by one.

Case A: $\mu_d > 0$, $\mu_i < m_i - m_{i+1}$ for some $i < d$.
In this case we apply the substitution $\mu_i \mapsto (\mu_i + 1)$, $\mu_d \mapsto (\mu_d - 1)$, which leads to the change

$$\delta F_2 = 2\bigl(-\mu_i + \mu_d + (d-i-1) + m_{i+1} - m_d\bigr) \geq 2\bigl(\mu_d + (d-i-1)\bigr) > 0$$

in the target functional. In this way we proceed until either all μ_i with $i < d$ satisfy the upper bound with equality (Case B below) or $\mu_d = 0$, i.e., Case C or Case D applies.

Case B: $\mu_d > 0$, $\mu_i = m_i - m_{i+1}$ for all $i < d$. In this case all μ_k, including μ_d are determined by the m_k and by the normalization ($\mu_d = N - m_1 + m_d$). Inserting these values into F_2, and using the normalization conditions, we get $F_2(\mathbf{m}, \mathbf{n}) = F_3(\mathbf{m}) - 2(M + dN) - N^2$ with

$$F_3(\mathbf{m}) = 2(N+d)m_1$$
$$\text{constrained by} \qquad m_1 \geq \cdots \geq m_d \geq 0 \ , \ \sum_k m_k = M, \qquad \text{and } m_1 - m_d \leq N.$$

This defines a variational problem in its own right. Any step increasing m_1 at the expense of some other m_k increases F_2. This process terminates either, when $M = m_1$, and all other $m_k = 0$. This is surely the case for $M < N$, because then $\mu_d = N - m_1 + m_d \geq N - M > 0$. This is already the final result claimed in the Lemma. On the other hand, the process may terminate because μ_d reaches 0 or would become negative. In the former case we get $\mu_d = 0$, and hence Case C or Case D. The latter case (termination at $\mu_d = 1$) may occur because the transformation $m_1 \mapsto (m_1 + 1)$, $m_d \mapsto (m_d - 1)$ changes $\mu_d = N - m_1 + m_d$ by -2. There are two basic situations in which changing both m_1 and m_d is the only option for maximizing F_3, namely $d = 2$ and $m_1 = m_2 = \cdots = m_d$. The first case is treated below as Case E. In the latter case we have $1 = N - m_1 + m_d = N$. Then the overall variational problem in the Lemma is trivial, because only one term remains, and one only has to maximize the quantity $2m_k - 2k - 1$, with trivial maximum at $k = 1$, $m_1 = M$.

Case C: $\mu_d = 0$, $m_d > 0$. For $\mu_d = 0$, the number m_d does not enter in the function F_2. Therefore, the move $m_d \mapsto 0$ and $m_1 \mapsto m_1 + m_d$, increases F_2 by $\mu_1 m_d \geq 0$. Note that this is always compatible with the constraints, and we end up in Case D.

Case D: $\mu_d = 0$, $m_d = 0$, $d > 2$. Set $d \mapsto (d-1)$. Note that we could now use the extra constraint $\mu_{d'} \leq m_{d'}$, where $d' = d - 1$. We will *not* use it, so in principle we might get a larger maximum. However, since we do find a maximizer satisfying all constraints, we still get a valid maximum.

Case E: $d = 2, \mu_1 = m_1 - m_2, \mu_2 = 1$. In this case $\mathbf{m} = (m_1, m_2)$ is completely fixed by the constraints. We have: $m_1 + m_2 = M$ and $\mu_1 + \mu_2 = m_1 - m_2 + 1 = N$ hence $m_1 - m_2 = N - 1$. This implies $2m_1 = M + N - 1$, $2m_2 = M - N + 1$ and since $m_2 \geq 0$ we get $M \geq N - 1$. If $M = N - 1$ holds we get $m_1 = N - 1 = M$, $m_2 = 0$ and consequently $\mu_1 = N - 1$. Together with $\mu_2 = 1 = N - M$ these are exactly the parameters where F_2 should take its maximum according to the Lemma. Hence assume $M \geq N$. In this case $\mu_2 = 1$ implies that F_2 becomes $NM - 3N - 4$, which is, due to $M \geq N$, strictly smaller than $F_2(M, 0; N, 0) = 2MN - N^2 - 2N$.

Uniqueness: In all cases just discussed the manipulations described lead to a strict increase of $F_2(\mathbf{m}, \mu)$ as long as $(\mathbf{m}, \mu) \neq (\mathbf{m}_{\max}, \mu_{\max})$ holds. The only exception is Case C with $\mu_1 = 0$. In this situation there is a $1 < k < d$ with $\mu_k > 0$. Hence we can apply the maps $d \mapsto d - 1$ (Case D) and $m_d \mapsto 0$ and $m_1 \mapsto m_1 + m_d$ (Case C) until we get $\mu_d \neq 0$ (i.e. d reaches k). Since $\mu_1 = 0$ the corresponding $(\mathbf{m}, \mu)$ is not equal to $(\mathbf{m}_{\max}, \mu_{\max})$. Therefore we can apply one of manipulations described in Case A, Case B or Case E which leads to a strict increase of $F_2(\mathbf{m}, \mu)$. This shows that $F_2(\mathbf{m}, \mu) < F_2(\mathbf{m}_{\max}, \mu_{\max})$ as long as $(\mathbf{m}, \mu) \neq (\mathbf{m}_{\max}, \mu_{\max})$ holds. Consequently the maximum is unique. **QED**.

With this result and the equations (21), (22), (24), (26) and (27) we can easily calculate $\omega_{\max}$:

$$\omega_{\max} = \omega(\widehat{T}) = \frac{M+d}{N+d}$$

and with (11) we get $\Delta(T) \geq \Delta(\widehat{T})$ with $\Delta(\widehat{T})$ from Theorem 1.

F. Proving uniqueness

One part of the uniqueness proof is already given above: there is only one optimal *covariant* cloning map, namely $\widehat{T}$. This follows easily from the uniqueness of the maximum found in Lemma 6 and from the fact that the representation π_N^+ is contained exactly once in the tensor product $\pi_M^+ \otimes \overline{\pi_{M-n}^+}$ (see equation A3 and the discussion in Subsection III C).

Suppose now that T is a non-covariant cloning map, which also attains the best value: $\Delta_{\text{one}}(T) = \Delta_{\text{one}}(\widehat{T})$. Then we may consider the average of $\overline{T}$ of T (see equation (6)), which is also optimal and, in addition, covariant. Therefore $\overline{T} = \widehat{T}$. The uniqueness part of the proof thus follows immediately from the following proposition:

7 Proposition. *Each completely positive, unital map $T : \mathcal{B}(\mathcal{H}^{\otimes M}) \to \mathcal{B}(\mathcal{H}_+^{\otimes N})$ satisfying the equation $\overline{T} = \widehat{T}$ equals $\widehat{T}$.*

Proof: We trace back this statement to the main theorem of [16]. To this end note that $\overline{T} = \widehat{T}$ implies the equivalent equation for the preduals:

$$\overline{T_*} = \int \tau_u T_* du = \widehat{T}_*$$

where τ_u acts on T_* by:

$$\tau_u T_*(\sigma) = \pi_\square^{\otimes M}(u)^* T_* \left(\pi_N^+(u)\sigma\pi_N^+(u)^*\right) \pi_\square^{\otimes M}(u).$$

Furthermore we know from the main theorem of [16] that $\operatorname{tr}\left(\sigma^{\otimes M} T_*(\sigma^{\otimes N})\right) \le \frac{d[N]}{d[M]}$ is true for all pure states $\sigma \in \mathcal{B}_*(\mathcal{H})$ and that equality holds iff $T = \widehat{T}$. Consequently we have

$$\int \left(\frac{d[N]}{d[M]} - \operatorname{tr}\left(\sigma^{\otimes M}\tau_u T(\sigma^{\otimes N})\right)\right) du = \frac{d[N]}{d[M]} - \operatorname{tr}\left(\sigma^{\otimes M}\overline{T_*}(\sigma^{\otimes N})\right) = \frac{d[N]}{d[M]} - \operatorname{tr}\left(\sigma^{\otimes M}\widehat{T}_*(\sigma^{\otimes N})\right) = 0.$$

Since the integral on the left hand site of this equation is taken over positive quantities the integrand has to vanish for all values of $u \in \mathrm{U}(d)$. This implies $\operatorname{tr}\left(\sigma^{\otimes M} T(\sigma^{\otimes N})\right) = \frac{d[N]}{d[M]}$ for all pure states $\sigma \in \mathcal{B}_*(\mathcal{H})$. However this is, according to [16], only possible if $T = \widehat{T}$. **QED**.

ACKNOWLEDGEMENTS

This paper is a response to the many discussions about the cloning problem one of us (R.F.W.) had with participants of the ISI Workshop on Quantum Computing in Torino in July 1997. We would like to thank D. Sondermann for a critical reading of the manuscript.

APPENDIX A: REPRESENTATIONS OF UNITARY GROUPS

Throughout this paper many arguments from representation theory of unitary groups are used. In order to fix the notation and to state the most relevant theorems we will recall in this appendix some well known facts from representation theory of Lie groups. General references are the books of Barut and Raczka [21], Zhelobenko [22] and Simon [17].

1. The groups and their Lie algebras

Let us consider first the group $\mathrm{U}(d)$ of all complex $d \times d$ unitary matrices. Its Lie algebra $\mathfrak{u}(d)$ can be identified with the Lie algebra of all anti-hermitian $d \times d$ matrices. The exponential function is then given by the usual matrix exponential $X \mapsto \exp(iX)$. $\mathfrak{u}(d)$ is a real Lie algebra. Hence we can consider its complexification $\mathfrak{u}(d) \otimes \mathbb{C}$ which coincides with the set of all $d \times d$ matrices and at the same time with the Lie algebra $\mathfrak{gl}(d, \mathbb{C})$ of the general linear group $\mathrm{GL}(d, \mathbb{C})$. In other words $\mathfrak{u}(d)$ is a real form of $\mathfrak{gl}(d, \mathbb{C})$. A basis of $\mathfrak{gl}(d, \mathbb{C})$ is given by the matrices $E_{jk} = |j\rangle\langle k|$.

The set of elements of $\mathrm{U}(d)$ with determinant one forms the subgroup $\mathrm{SU}(d)$ of $\mathrm{U}(d)$. Its Lie algebra $\mathfrak{su}(d)$ is the subalgebra of $\mathfrak{u}(d)$ consisting of the elements with zero trace. Hence the complexification $\mathfrak{su}(d) \otimes \mathbb{C}$ of $\mathfrak{su}(d)$ is the Lie algebra of trace-free matrices and coincides therefore with the Lie algebra $\mathfrak{sl}(d, \mathbb{C})$ of the special linear group $\mathrm{SL}(d, \mathbb{C})$. As well as in the $\mathrm{U}(d)$ case this means that $\mathfrak{su}(d)$ is a real from of $\mathfrak{sl}(d, \mathbb{C})$. The matrices E_{jk} are no longer a basis for $\mathfrak{sl}(d, \mathbb{C})$ since the E_{jj} are not trace free. Instead we have to consider E_{jk}, $j \neq k$ and $H_j = E_{jj} - E_{j+1,j+1}$, $j = 1, \ldots, d-1$. The difference between $\mathfrak{sl}(d, \mathbb{C})$ and $\mathfrak{gl}(d, \mathbb{C})$ is exactly the center of $\mathfrak{gl}(d, \mathbb{C})$, i.e. all complex multiples of the identity matrix. In other words we have $\mathfrak{gl}(d, \mathbb{C}) = \mathfrak{sl}(d, \mathbb{C}) \oplus \mathbb{C}\mathbb{1}$. A similar result holds for the real forms: $\mathfrak{u}(d) = \mathfrak{su}(d) \oplus \mathbb{R}\mathbb{1}$.

The (real) span of all iE_{jj}, $j = 1, \ldots, d$ is a subalgebra of $\mathfrak{u}(d)$ which is maximal abelian, i.e. a Cartan subalgebra of $\mathfrak{u}(d)$. We will denote it in the following by $\mathfrak{t}(d)$ and its complexification by $\mathfrak{t}_{\mathbb{C}}(d) \subset \mathfrak{gl}(d, \mathbb{C})$. The intersection of $\mathfrak{t}(d)$ with $\mathfrak{su}(d)$ results in a Cartan subalgebra $\mathfrak{st}(d)$ of $\mathfrak{su}(d)$. We will denote the complexification by $\mathfrak{st}_{\mathbb{C}}(d)$. Again the two algebras $\mathfrak{t}(d)$ and $\mathfrak{st}(d)$ differ by the center of $\mathfrak{u}(d)$ i.e. $\mathfrak{t}(d) = \mathfrak{st}(d) \oplus \mathbb{R}\mathbb{1}$ and $\mathfrak{t}_{\mathbb{C}}(d) = \mathfrak{st}_{\mathbb{C}}(d) \oplus \mathbb{C}\mathbb{1}$ in the complexified case.

2. Representations

Consider now a finite-dimensional[2] representation $\pi : \mathrm{U}(d) \to \mathrm{GL}(N, \mathbb{C})$ of $\mathrm{U}(d)$. It is characterized uniquely by the corresponding representation $\partial\pi : \mathfrak{u}(d) \to \mathfrak{gl}(N, \mathbb{C})$ of its Lie algebra, i.e. we have $\pi(\exp(X)) = \exp(\partial\pi(X))$. The representation $\partial\pi$ can be extended by complex linearity to a representation of $\mathfrak{gl}(d, \mathbb{C})$ which we will denote by $\partial\pi$ as well. Hence $\partial\pi$ leads to a representation π of the group $\mathrm{GL}(d, \mathbb{C})$. Similar notations we will adopt for representations of $\mathrm{SU}(d)$ and $\mathrm{SL}(d, \mathbb{C})$.

Assume now that π is an irreducible representation of $\mathrm{GL}(d, \mathbb{C})$. An infinitesimal weight of π (or simply a weight in the following) is an element λ of the dual of $\mathfrak{t}^*_{\mathbb{C}}(d)$ of $\mathfrak{t}_{\mathbb{C}}(d)$ such that $\partial\pi(X)x = \lambda(X)x$ holds for all $X \in \mathfrak{t}_{\mathbb{C}}(d)$ and for a nonvanishing $x \in \mathbb{C}^N$. The linear subspace $V_\lambda \subset \mathbb{C}^N$ of all such x is called the weight subspace of the weight λ. The set of weights of π is not empty and, due to irreducibility, there is exactly one weight $\mathbf{m}$, called the highest weight, such that $\partial\pi(E_{jk})x = 0$ for all x in the weight subspace of $\mathbf{m}$ and for all $j, k = 1, \ldots, d$ with $j < k$. The representation π is (up to unitary equivalence) uniquely determined by its highest weight. On the other hand the weight $\mathbf{m}$ is uniquely determined by its values $\mathbf{m}(E_{jj}) = m_j$ on the basis E_{jj} of $\mathfrak{t}_{\mathbb{C}}(d)$. We will express this fact in the following as "$\mathbf{m} = (m_1, \ldots, m_d)$ is the highest weight of the representation π". For each analytic representation of $\mathrm{GL}(d, \mathbb{C})$ the m_j are integers satisfying the inequalities $m_1 \geq m_2 \geq \ldots \geq m_d$ and the converse is also true: each family of integers with this property defines the highest weight of an analytic, irreducible representation of $\mathrm{GL}(d, \mathbb{C})$.

In a similar way we can define weights and highest weights for representations of the group $\mathrm{SL}(d, \mathbb{C})$ as linear forms on the Cartan subalgebra $\mathfrak{st}_{\mathbb{C}}(d)$. As in the $\mathrm{GL}(d, \mathbb{C})$-case an irreducible representation π of $\mathrm{SL}(d, \mathbb{C})$ is characterized uniquely by its highest weight $\mathbf{m}$. However we can not evaluate $\mathbf{m}$ on the basis E_{jj} since these matrices are not trace free. One possibility is to consider an arbitrary extension of $\mathbf{m}$ to the algebra $\mathfrak{t}_{\mathbb{C}}(d) = \mathfrak{st}_{\mathbb{C}}(d) \oplus \mathbb{C}\mathbb{1}$. Obviously this extension is not unique. Therefore the values $\mathbf{m}(E_{jj}) = m_j$ are unique only up to an additive constant. To circumvent this problem we will use usually the normalization condition $m_d = 0$. In this case the integer m_j corresponds to the number of boxes in the j^{th} row of the Young tableau usually used to characterize the irreducible representation π. Another possibility to describe the weight $\mathbf{m}$ is to use the basis H_j of $\mathfrak{st}_{\mathbb{C}}(d)$. We get a sequence of integers $l_j = \mathbf{m}(H_j)$, $j = 1, \ldots, d-1$. They are related to the m_j by $l_j = m_j - m_{j+1}$. Each sequence $l_1, \ldots, l_{d-1}$ defines the highest weight of an irreducible representation of $\mathrm{SL}(d, \mathbb{C})$ iff the l_j are positive integers.

Finally consider the representation $\overline{\pi}$ conjugate to π, i.e. $\overline{\pi}(u) = \overline{\pi(u)}$. If π is irreducible the same is true for $\overline{\pi}$. Hence $\overline{\pi}$ admits a highest weight which is given by $(-m_d, -m_{d-1}, \ldots, -m_1)$. If π is a $\mathrm{SU}(d)$ representation we can apply the normalization $m_d = 0$. Doing this as well for the conjugate representation we get $(m_1, m_1 - m_{d-1}, \ldots, m_1 - m_2, 0)$. In terms of Young tableaus this corresponds to the usual rule to construct the tableau of the conjugate representation: Complete the Young tableau of π to form a $d \times m_1$ rectangle. The complementary tableau rotated by $180°$ is the Young tableau of $\overline{\pi}$.

[2] All representations in this paper are finite dimensional.

3. Tensor products of representations

Consider now two finite dimensional irreducible representations $\pi_{\mathbf{m}}, \pi_{\mathbf{n}}$ of $\mathrm{U}(d)$ with highest weights $\mathbf{m}, \mathbf{n}$. Their tensor product $\pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}}$ is completely reducible. If r_π denotes the multiplicity of the irreducible representation π in $\pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}}$ then this means that $\pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}} = \bigoplus_\pi r_\pi \pi$. Hence to decompose the representation $\pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}}$ we have to compute the integer valued functions $(\mathbf{m}, \mathbf{n}) \mapsto r_\pi(\mathbf{m}, \mathbf{n})$. There are several general schemes to do this (see e.g. [22, Ch. XII]). However we are only interested in the following special cases. The highest weight of the representation $\pi_{\mathbf{1}} : \mathrm{U}(d) \ni U \mapsto U \in \mathrm{GL}(d, \mathbb{C})$ (denoted $\pi_\square$ in Section III A) is $\mathbf{1} = (1, 0, \ldots, 0)$. Consider the $N-$fold tensor product of this representation It can be decomposed as follows

$$\pi_{\mathbf{1}}^{\otimes N} = \sum_{\substack{m_1+\ldots+m_d=N \\ m_d \geq 0}} r(m_1, \ldots, m_d) \pi_{m_1,\ldots,m_d} \tag{A1}$$

where $\pi_{m_1,\ldots,m_d}$ denotes the irreducible representation with highest weight $(m_1, \ldots, m_d)$. The coefficients $r(m_1, \ldots, m_d)$ are determined by the following recurrence relation:

$$r(m_1, \ldots, m_d) = r(m_1 - 1, \ldots, m_d) + r(m_1, m_2 - 1, \ldots, m_d) + \ldots + r(m_1, \ldots, m_d - 1). \tag{A2}$$

Consider now the $N-$fold symmetric tensor product of $\pi_{\mathbf{1}}$ (denoted π_N^+ in Section III A). It is irreducible with highest weight $N\mathbf{1} = (N, 0, \ldots, 0)$ (hence $\pi_N^+ = \pi_{N\mathbf{1}}$). The tensor product of this representation with an arbitrary irreducible representation $\pi_{\mathbf{m}}$ (with highest weight $\mathbf{m} = (m_1, \ldots, m_d)$) is

$$\pi_{N\mathbf{1}} \otimes \pi_{\mathbf{m}} = \sum_{\substack{0 \leq \mu_{k+1} \leq m_k - m_{k+1} \\ \mu_1+\ldots+\mu_d=N}} \pi_{m_1+\mu_1,\ldots,m_d+\mu_d}. \tag{A3}$$

From this equation we also get a condition for $\pi_{N\mathbf{1}}$ to be contained in an arbitrary tensor product $\pi_{\mathbf{m}} \otimes \pi_{\mathbf{n}}$ which we need in Section III E: For arbitrary weights $\mathbf{m}, \mathbf{n}, \mathbf{p}$ we have

$$\pi_{\mathbf{m}} \subset \pi_{\mathbf{n}} \otimes \pi_{\mathbf{p}} \iff \pi_{\mathbf{n}} \subset \overline{\pi_{\mathbf{p}}} \otimes \pi_{\mathbf{m}} \tag{A4}$$

If two irreducible representations $\pi_{\mathbf{m}}, \pi_{\mathbf{n}}$ of $\mathrm{SU}(d)$ are given we can characterize them, as described above, by their highest weights $\mathbf{m} = (m_1, \ldots, m_d)$ and $\mathbf{n} = (n_1, \ldots, n_d)$ using the normalizations $m_d = 0$ and $n_d = 0$. After applying the stated theorems to the tensor product of the corresponding $\mathrm{U}(d)$ representations we can restrict the summands in the resulting spectral decomposition back to $\mathrm{SU}(d)$, i.e. we renormalize the heighest weigths $(m_1, \ldots, m_d)$ to the $m_d = 0$ case.

4. Nondegeneracy of $\mathfrak{su}(d)$

We are now ready to discuss the group theoretic part of the proof of our main theorem, i.e. Lemma 3 which we have only stated in Section III. According to Def. 2 we have to show that each linear operator $\Lambda : \mathfrak{su}(d) \to \mathcal{H}_+^{\otimes N}$ with the covariance property

$$\pi_N^+(g)\Lambda(X)\pi_N^+(g^{-1}) = \Lambda(gXg^{-1}) \tag{A5}$$

is of the form $\Lambda(X) = \lambda \partial\pi_+^N(X)$ with a constant factor λ. Here π_N^+ is the irreducible representation of $\mathrm{SU}(d)$ introduced in Section III A. (Hence we have $\pi_N^+ = \pi_{N\mathbf{1}}$ using the notation introduced in Subsection A 3 of this appendix.)

To reformulate this statement note first that the map $g \mapsto \pi_N^+(g) \cdot \pi_N^+(g^{-1})$ can be interpreted as a unitary representation of $\mathrm{SU}(d)$ on the representation space $\mathcal{H}_+^{\otimes N} \otimes \mathcal{H}_+^{\otimes N}$. In fact it is (unitarily equivalent to) the tensor product $\pi_N^+ \otimes \overline{\pi_N^+}$. Since $\mathrm{SU}(d) \ni g \mapsto g \cdot g^{-1} \in \mathcal{B}(\mathfrak{su}(d))$ is the adjoint representation of $\mathrm{SU}(d)$ this implies that each map X satisfying (A5) intertwines $\pi_N^+ \otimes \overline{\pi_N^+}$ and the adjoint representation Ad. Note second that the representation $\partial\pi_N^+$ of the Lie algebra $\mathfrak{su}(d)$ satisfies equation (A5) in an obvious way (with $\lambda = 1$) hence we have to show that all such intertwiners are proportional, or in other words that Ad is contained in $\pi_N^+ \otimes \overline{\pi_N^+}$ exactly once.

Let us discuss now the tensor product $\pi_N^+ \otimes \overline{\pi_N^+}$. The irreducible representation π_N^+ has highest weight $(N, 0, \ldots, 0)$ (see Section A 2) and consequently the highest weight of its conjugate is $(N, \ldots, N, 0)$. We can apply now equation (A3) which shows that the adjoint representation whose highest weight is $(2, 1, \ldots, 1, 0)$ is contained in $\pi_N^+ \otimes \overline{\pi_N^+}$ exactly ones. This shows together with our previous discussion that $\mathfrak{su}(d)$ is nondegenerate in $\mathcal{H}_+^{\otimes N}$ with respect to π_N^+.

5. The Casimir invariants

To each Lie algebra $\mathfrak{g}$ we can associate its universal enveloping algebra $\mathfrak{G}$. It is defined as the quotient of the full tensor algebra $\bigoplus_{n\in\mathbb{N}_0}\mathfrak{g}^{\otimes N}$ with the two sided ideal $\mathfrak{I}$ generated by $X\otimes Y - Y\otimes X - [X,Y]$, i.e. $\mathfrak{G}$ is an associative algebra. The original Lie algebra $\mathfrak{g}$ can be embedded in its envelopping algebra $\mathfrak{G}$ by $\mathfrak{g}\ni X\mapsto X+\mathfrak{I}\in\mathfrak{G}$. The Lie bracket is then simply given by $[X,Y]=XY-YX$. Moreover $\mathfrak{G}$ is algebraically generated by $\mathfrak{g}$ and $\mathbb{1}$. Hence each representation $\partial\pi$ of $\mathfrak{g}$ generates a unique representation $\partial\pi$ of $\mathfrak{G}$ simply by $\partial\pi(X_1\cdots X_k)=\partial\pi(X_1)\cdots\partial\pi(X_k)$. If $\partial\pi$ is irreducible the induced representation $\partial\pi$ is irreducible as well.

We are interested not in the whole algebra but only in its center $\mathfrak{Z}(\mathfrak{G})$, i.e. the subalgebra consisting of all $Z\in\mathfrak{G}$ commuting with all elements of $\mathfrak{G}$. The elements of $\mathfrak{Z}(\mathfrak{G})$ are called central elements or Casimir elements. If $\partial\pi$ is a representation of $\mathfrak{G}$ the representatives $\partial\pi(Z)$ of Casimir elements commute with all other representatives $\partial\pi(X)$. This implies for irreducible representations that all $\partial\pi(Z)$ are multiples of the identity.

Consider now the case $\mathfrak{g}=\mathfrak{gl}(d,\mathbb{C})$. In this case we can identify the envelopping algebra $\mathfrak{G}$ with the set of all left invariant differential operators on $\mathrm{GL}(d,\mathbb{C})$ (a similar statement is true for any Lie group). Of special interest for us are the Casimir elements belonging to operators of first and second order. Using the standard basis E_{ij} of $\mathfrak{gl}(d,\mathbb{C})$ introduced in Section A 1 they are given by

$$\mathbf{C}_1=\sum_{j=1}^{d}E_{jj}\ \text{and}\ \mathbf{C}_2=\sum_{j,k=1}^{d}E_{jk}E_{kj}.$$

Of course $\mathbf{C}_1^2$ is as well of second order and it is linearly independent of $\mathbf{C}_2$. Hence each second order Casimir element of $\mathfrak{G}$ is a linear combination of $\mathbf{C}_2$ and $\mathbf{C}_1^2$.

If $\partial\pi$ is an irreducible representation of $\mathfrak{gl}(d,\mathbb{C})$ with highest weight $(m_1,\dots,m_d)$ it induces, as described above, an irreducible representation $\partial\pi$ of $\mathfrak{G}$ and the images of $\partial\pi(\mathbf{C}_1)$ and $\partial\pi(\mathbf{C}_2)$ are multiples of the identity, i.e. $\partial\pi(\mathbf{C}_1)=C_1(\pi)\mathbb{1}$ and $\partial\pi(\mathbf{C}_2)=C_2(\pi)\mathbb{1}$ with

$$C_1(\pi)=\sum_{j=1}^{d}m_j\ \text{and}\ C_2(\pi)=\sum_{j=1}^{d}m_j^2+\sum_{j<k}(m_j-m_k). \tag{A6}$$

Let us discuss now the Casimir elements of $\mathrm{SL}(d,\mathbb{C})$. Since $\mathrm{SL}(d,\mathbb{C})$ is a subgroup of $\mathrm{GL}(d,\mathbb{C})$ its enveloping algebra $\mathfrak{S}$ is a subalgebra of $\mathfrak{G}$. However the corresponding Lie algebras differ only by the center of $\mathfrak{gl}(d,\mathbb{C})$. Hence the center $\mathfrak{Z}(\mathfrak{S})$ of $\mathfrak{S}$ is a subalgebra of $\mathfrak{Z}(\mathfrak{G})$. Since $\mathfrak{sl}(d,\mathbb{C})$ is simple there is no first order Casimir element and there is only one second order Casimir element $\widetilde{\mathbf{C}}_2$ which is therefore a linear combination $\widetilde{\mathbf{C}}_2=\mathbf{C}_2+\alpha\mathbf{C}_1^2$ of $\mathbf{C}_1^2$ and $\mathbf{C}_2$. Obviously the factor α is uniquely determined by the condition that the expression

$$\widetilde{C}_2(\pi)=C_1(\pi)+\alpha C_1^2(\pi)=\sum_{j=1}^{d}m_j^2+\sum_{j<k}(m_j-m_k)+\alpha\left(\sum_{j=1}^{d}m_j\right)^2 \tag{A7}$$

with $\partial\pi(\widetilde{\mathrm{C}}_2)=\widetilde{C}_2(\pi)\mathbb{1}$ is invariant under the renormalization $(m_1,\dots,m_d)\mapsto(m_1+\mu,\dots,m_d+\mu)$ with an arbitrary constant μ. Straightforward calculations show that $\alpha=-\frac{1}{d}$. Hence we get $\widetilde{C}_2=C_2-\frac{1}{d}C_1^2$ and

$$\widetilde{C}_2(\pi)=\frac{1}{d}\left((d-1)\sum_{j=1}^{d}m_j^2-\sum_{j\neq k}^{d}m_jm_k+d\sum_{j<k}(m_j-m_k)\right). \tag{A8}$$

Alternatively $\widetilde{\mathbf{C}}_2$ can be expressed in terms of a basis $(X_j)_j$ of $\mathfrak{sl}(d,\mathbb{C})$. In fact there is a symmetric second rank tensor $g^{jk}X_j\otimes X_k\in\mathfrak{sl}(d,\mathbb{C})\otimes\mathfrak{sl}(d,\mathbb{C})$ such that $\widetilde{\mathbf{C}}_2$ coincides with the equivalence class of g^{jk} in $\mathfrak{S}$. In other words $\widetilde{\mathbf{C}}_2=\sum_{jk}g^{jk}X_jX_k$ holds which leads to

$$\widetilde{C}_2(\pi)\mathbb{1}=\sum_{jk}g^{jk}\partial\pi(X_i)\partial\pi(X_j) \tag{A9}$$

for an irreducible representation π of $\mathrm{SU}(d)$.

APPENDIX B: STINESPRING THEOREM FOR COVARIANT CP-MAPS

In this appendix we will state the covariant version of Stinespring's theorem [19] which we have used in the proof of Theorem 1. However, as in the rest of the paper, we will restrict the discussion to finite dimensional Hilbert spaces (i.e. only cp-maps between finite von Neumann factors are considered).

8 Theorem. *Let G be a group with finite dimensional unitary representations $\pi_i : G \to \mathcal{B}(\mathcal{H}_i)$ $(i = 1, 2)$, and $T : \mathcal{B}(\mathcal{H}_2) \to \mathcal{B}(\mathcal{H}_1)$ a completely positive map with the covariance property $\pi_1(g)T(X)\pi_1(g)^* = T(\pi_2(g)X\pi_2(g)^*)$.*

1. *Then there is another finite dimensional unitary representation $\tilde{\pi} : G \to \mathcal{B}(\tilde{\mathcal{H}})$ and an intertwiner $V : \mathcal{H}_1 \to \mathcal{H}_2 \otimes \tilde{\mathcal{H}}$ with $V\pi_1(g) = \pi_2 \otimes \tilde{\pi} V$ such that $T(X) = V^*(X \otimes \mathbb{1})V$ holds.*
2. *If $T = \sum_\alpha T^\alpha$ is a decomposition of T in completely positive terms, there is a decomposition $\mathbb{1} = \sum_\alpha F^\alpha$ of the identity operator on $\tilde{\mathcal{H}}$ into positive operators $F^\alpha \in \mathcal{B}(\tilde{\mathcal{H}})$ with $[F^\alpha, \tilde{\pi}(g)] = 0$ such that $T^\alpha(X) = V^*(X \otimes F^\alpha)V$*

We only sketch the main ideas of the proof. The first step is Stinespring's theorem in its general form [18]: There exists a representation $\eta : \mathcal{B}(\mathcal{H}_2) \to \mathcal{B}(\mathcal{K})$ of the C*-algebra $\mathcal{B}(\mathcal{H}_2)$ on a Hilbert space $\mathcal{K}$ and a bounded operator $V : \mathcal{H}_1 \to \mathcal{K}$ such that $T(X) = V^*\eta(X)V$ holds. Up to unitary equivalence there is exactly one such triple $(\mathcal{K}, V, \pi)$ such that the vectors $\pi(A)V\psi \in \mathcal{K}$ with $\psi \in \mathcal{H}_1$ and $A \in \mathcal{B}(\mathcal{H}_2)$ span $\mathcal{K}$.

It is this uniqueness, from which the representation $\tilde{\pi}$ of G is constructed. Indeed, the objects $V_g = V\pi_1(g)$, and $\eta_g(X) = \eta(\pi_2(g)X\pi_2(g)^*)$ form a Stinespring dilation of the completely positive map $T_g(X) = \pi_1(g)^*T(\pi_2(g)X\pi_2(g)^*)\pi_1(g)$, which by covariance is equal to T. Hence by "uniqueness up to unitary equivalence" there is a unique unitary operator $U_g \in \mathcal{B}(\mathcal{K})$ such that $V_g = V\pi_1(g) = U_gV$, and $\eta_g(X) = \eta(\pi_2(g)X\pi_2(g)^*) = U_g\eta(X)U_g^*$. This can be simplified a bit further by the observation that according to the second equation the operators $\tilde{U}_g = \eta(\pi_2(g))^*U_g$ commute with all $\eta(X)$. It is easy to see that the U_g are a representation, and hence so is $\tilde{U}$: we have $\tilde{U}_g\tilde{U}_h = \eta(\pi_2(g))^*U_g\eta(\pi_2(h)^*)U_h = \eta(\pi_2(g))^*\eta(\pi_2(g)\pi_2(h)^*\pi_2(g)^*)U_gU_h = \eta(\pi_2(g)^*\pi_2(g)\pi_2(h)^*\pi_2(g)^*)U_{gh} = \eta(\pi_2(gh)^*)U_{gh} = \tilde{U}_{gh}$.

For a proof of part (1) we now only need to invoke the observation that all representations of $\mathcal{B}(\mathcal{H}_2)$ are of the form $\eta \simeq \mathrm{id} \otimes \mathbb{1}$ with $\mathcal{K} = \mathcal{H}_2 \otimes \tilde{\mathcal{H}}$. (Here "$\simeq$" denotes a unitary equivalence, which we will include as a factor in V. Since $\tilde{U}_g$ commutes with all $\eta(X) = X \otimes \mathbb{1}$, it is of the form $\tilde{U}_g = \mathbb{1} \otimes \tilde{\pi}(g)$, which proves the assertion.

The second part of the theorem stated for a trivial group $G = \{e\}$ is also known as the Radon-Nikodyn theorem coming with the Stinespring theorem. In general it asserts the existence of a partition of the identity operator on $\mathcal{K}$ into operators $\tilde{F}^\alpha$ commuting with all $\eta(X)$, giving the decomposition of T as $T^\alpha = V^*\eta(X)F^\alpha V$. Again, we can write these as $\tilde{F}^\alpha = \mathbb{1} \otimes F^\alpha$. Since the $F^\alpha V$ are uniquely determined by the T^α, it is easy to see that covariance of T^α is equivalent to $F^\alpha = \tilde{\pi}_g F^\alpha \tilde{\pi}_g^*$.

---

[1] W.K. Wootters and W.H. Zurek, "A single quantum cannot be cloned" Nature **299**, 802 (1982).
[2] V. Bužek and M. Hillery, "Quantum copying: beyond the no-cloning theorem" `quant-ph/9607018` Phys.Rev. A **54**, 1844 (1996).
[3] M. Hillery and V. Bužek, "Quantum copying: Fundamental inequalities" Phys.Rev. A **56**, 1212 (1997).
[4] N. Gisin and S. Massar, "Optimal quantum cloning machines" `quant-ph/9705046` Phys.Rev.Lett. **79**, 2153 (1997).
[5] D. Bruß, D.P. DiVincenzo, A. Ekert, C.A. Fuchs, C. Machiavello, and J.A. Smolin, "Optimal universal and state-dependent cloning", Report Los Alamos, `quant-ph/9705038` Phys. Rev. A **57**, 2368 (1998).
[6] D. Bruß, A. Ekert, and C. Machiavello, "Optimal universal cloning and state estimation", Report Los Alamos, `quant-ph/9712019`
[7] V. Bužek and M. Hillery, "Universal optimal cloning of qubits and quantum registers", Report Los Alamos, `quant-ph/9801009`
[8] P. Zanardi, "A Note on Quantum Cloning in d dimensions", Report Los Alamos, `quant-ph/9804011`
[9] N. Gisin and B. Huttner, "Quantum cloning, eavesdropping and Bell's inequality" Phys.Lett. A **228**, 13 (1997).
[10] N. Gisin, "Quantum cloning without signaling" Report Los Alamos, `quant-ph/9801005`
[11] T. Mor, "No-cloning of Orthogonal States in Composite Systems", Report Los Alamos, `quant-ph/9802036`
[12] N. J. Cerf, "Quantum cloning and the capacity of the Pauli channel", Report Los Alamos, `quant-ph/9803058`
[13] N. J. Cerf, "Asymmetric quantum cloning machines", Report Los Alamos, `quant-ph/9805024`
[14] Chi-Sheng Niu and R. B. Griffiths, "Optimal copying of one quantum bit", Report Los Alamos, `quant-ph/9805073`

[15] M. Murao, D. Jonathan, M. B. Plenio and V. Vedral, "Quantum telecloning and multiparticle entanglement", Report Los Alamos, quant-ph/9806082

[16] R.F. Werner, "Optimal cloning of pure states Report Los Alamos, quant-ph/9804001 To appear in *Phys.Rev.A*

[17] B. Simon, "Representations of finite and compact groups", Amer. Math. Soc. (1996)

[18] W.F. Stinespring, "Positive functions on C*-algebras" Proc.Amer.Math.Soc. **6**, 211 (1955).

[19] H. Scutaru, "Some remarks on covariant completely positive linear maps on C*-algebras", Rep. Math. Phys. **16**, 79-87 (1979)

[20] M. Fannes, B. Nachtergaele, and R.F. Werner, "Exact antiferromagnetic ground states of quantum spin chains" Europhys.Lett. **10**, 633 (1989)

[21] A. O. Barut and R. Raczka, "Theory of group representations and applications", World Scientific (1986)

[22] D. P. Zhelobenko, "Compact Lie groups and their representations", Amer. Math. Soc (1978)